Microsoft 365 Defender - konfigurácia, správa a detekcia incidentov

Kód kurzu: GOC250

Päťdňový pokročilý kurz je určený bezpečnostným špecialistom, administrátorom, blue team analytikom a SOC, ktorí chcú efektívne využívať celý ekosystém Microsoft Defender ako jednotnú platformu na prevenciu, detekciu, vyšetrovanie a reakciu na bezpečnostné incidenty. Kurz pokrýva kompletný Microsoft Defender XDR stack vrátane Defender for Endpoint, Defender for Office 365, Defender for Cloud a Defender for Cloud Apps. Kurz detailne rozoberá konfiguráciu a správu jednotlivých komponentov Microsoft Defender XDR, ich vzájomnú integráciu a praktické využitie pri detekcii moderných kybernetických hrozieb. Účastníci získajú hlbšie porozumenie útokom zameraným na identity, endpointy, elektronickú poštu a cloudové aplikácie a naučia sa, ako pomocou Microsoft Defender technológií tieto útoky mitigovať alebo včas detekovať. Súčasťou kurzu je aj analýza vyšetrovania incidentov a advanced hunting.

Predpokladané vstupné znalosti

Povedomie a základné znalosti v rozsahu kurzov uvedených v sekciách Predchádzajúce kurzy a Súvisiace kurzy

Osnova kurzu

Microsoft Defender XDR

- Architektúra Microsoft Defender XDR
- Integrácia jednotlivých Defender komponentov
- RBAC a riadenie prístupu

Defender for Endpoint

- Nasadenie a konfigurácia
- Endpoint Detection and Response (EDR)
- Attack Surface Reduction
- Vulnerability Management
- Device Investigation
- Automated Investigation and Remediation

Defender for Office 365

- Ochrana elektronickej pošty
- Anti-Phishing a Anti-Spam ochrana
- Safe Links a Safe Attachments
- Threat Explorer

Defender for Cloud

- Architektúra a konfigurácia
- CSPM a Secure Score
- Ochrana cloudových workloadov
- Integrácia s Defender XDR
- Detekcia a vyšetrovanie hrozieb v cloude

Defender for Cloud Apps

- SaaS Security
- Shadow IT a Discovery
- App Risk Assessment
- Access a Session Policies
- Cloud Threat Detection
- Vyšetrovanie kompromitovaných cloudových aplikácií

Threat Detection &Incident Response

- Vyšetrovanie incidentov
- KQL základy

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

- Advanced Hunting
- Response Actions a Remediation

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved